## REMARKS

Status of the Claims:

Claims 1-39 are now pending;

Claims 1-39 have been rejected;

Claim 1, 3-9, 12-13, 19, 21-27, and 30-31 have been amended;

Claims 18 and 36-39 have been canceled;

Claims 2, 10-11, 14-17, 20, 28-29, 32-35 are original.

Introduction

In the Office Action, portions of the specification were objected to because of certain informalities. By the foregoing amendments, these informalities have now been corrected.

Claims 3-9, 12-17, 21-35, and 38 were rejected under 35 U.S.C. § 112, ¶2, as allegedly indefinite.

Claims 1-39 were rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent App. Pub. 2003/0135762 by Macaulay (hereinafter "Macaulay").

Objection to the Specification and rejection of Claims 3-7, 21-25, and 38 under 35 U.S.C. § 112, ¶2 due to references to "IEEE Standard 802.11"

The Examiner has objected to the incorporation by reference of "IEEE Standard 802.11" in the Specification as not clearly disclosing which version of the standard is to be incorporated. The reference to "IEEE Standard 802.11" in the Specification has been amended to refer to "IEEE Standards 802.11a/b/g," all of which were in effect on the date of the filing of the application. One of ordinary skill in the art would have understood that a generic reference

-10-

to "IEEE Standard 802.11" in the context of wireless LAN security referred to amendments

802.11a, 802.11b, and 802.11g, all of which were in effect on the date of the filing of the

application. References to "IEEE Standard 802.11" in the claims have been similarly amended

to read "IEEE Standard 802.11 a/b/g," referring to the 802.11a, 802.11b, and 802.11g standards.

Rejection of Claims 13 and 31 under 35 U.S.C. § 112, ¶2

Claims 13 and 31 have been amended to more clearly describe the "More Data"

field.

Rejections under 35 U.S.C. § 102(e)

In the Office Action, claims 1-39 were rejected under 35 U.S.C. § 102(e) as

allegedly anticipated by Macaulay. Claims 36-39 have been canceled, and independent claims 1

and 19 amended to better define the differences between the present invention and the prior art.

Applicant respectfully traverses the rejections of record.

Amended independent claims 1 and 19 are directed to methods for unauthorized

access attempts to a wireless system, including, *inter alia*,

> maintaining a state table on said computer, said state table storing state
> information for said mobile units; and

> operating said computer to compare format and state information of said one or
> more received data packets to selected requirements of said protocol-specified
> format and said stored state information

The Examiner alleges that Macaulay discloses or suggests these claim limitations

at paragraphs 0043-0046; 0090; 0095-0107; and paragraphs 0032-0035 and 0042. Applicants

respectfully disagree. The cited portions of Macaulay fail to disclose at least maintaining a state

table and comparing the format and state information of received data packets to a protocol-

specified format and state information stored in the state table. For at least this reason, Macaulay cannot anticipate amended independent claims 1 and 19.

Macaulay is directed to "a wireless security system ... [that] enables users to detect and neutralize unauthorized or defective 802.11 devices and pin-points their physical location..." (Macaulay, para. 0010). The system is designed to detect a variety of intrusion attempts into wireless networks, including devices masquerading as authorized devices by assuming their IP addresses. (*See Id.*, para 0101-0102). The system maintains log files of data collected by a "Listening Post Module" from wireless devices on the network, which the Examiner has cited as an example of the state table of the current invention. (*See* Office Action, page 6; *Id.*, para 0090-0091).

However, these log files are not utilized by the system of Macaulay in any way. Rather, the log files are stored "with a specific intent of supporting analysis and display by third-party Analysis Products." (*Id.*, para. 0091). Such Third-party Analysis Products include "intrusion detection system tools or database tools for reporting." (*Id.*, para. 0044). This can be further seen in Figure 2 of Macaulay, wherein log files (220), once stored, are transmitted only to the third-party analysis product (260), and are not further utilized by the system. (*See Id.*, Fig. 2). The system of Macaulay is designed to detect a number of attacks, as cited by the Examiner in the Office Action, looking for failed access attempts, jamming (emitting "copious or extraneous IEEE 802.11 frames), sabotage (emitting "IEEE 802.11 management or control frames"), and the like. However, the only review of stored data by Analysis module (230) when attempting to detect threats is the checking of MAC addresses for duplicate or changed addresses.

In contrast, independent claims 1 and 19 relate to comparing the state information

of received data packets to state information stored in a state table to detect unauthorized access to the wireless network. For instance, if the WEP flag of an incoming packet with an authorized MAC address is inconsistent with flag value stored in the state table for that MAC address, it may indicate a possible network intrusion attempt, and an alarm may be generated. (*See* Specification, para. 0022). Similarly, if the protocol version field of the Frame Control field of a packet is different from that stored in the state table for that mobile device or access point, an intrusion attempt may be underway. (*Id.*, para 0023). Many different state information variables are stored in the state table, and each incoming packet is checked for inconsistencies. (*See Id.*, para. 0022-0028).

As previously discussed, the portions of Macaulay cited by the Examiner for this proposition refer only to the storage and checking of MAC addresses. (*See* Office Action, p. 7; Macaulay, para. 0101 and 0102). Such a system is vulnerable to intrusion attempts wherein the intruder "spoofs" the MAC address of an authorized mobile device or access point, whereas the method of claims 1 and 19 could detect such an intrusion attempt by comparing the state information of packets transmitted to that stored in the state table. (*See* Specification, para. 0025-0026).

For at least these reasons, Applicant respectfully submits that amended claims 1 and 19 are allowable over Macaulay. Since claims 2-17 and 20-35 depend from claims 1 and 19, respectively, Applicant also respectfully submits that they are in condition for allowance.

## CONCLUSION

In view of the foregoing remarks, favorable reconsideration and allowance of claims 1-17 and 19-35 are respectfully solicited. In the event that the application is not deemed in condition for allowance, the Examiner is invited to contact the undersigned in an effort to advance the prosecution of this application.

Respectfully submitted,

Robert L. Maier
Patent Office Reg. No. 54,291
(212) 408-2538

Robert C. Scheinfeld
Patent Office Reg. No. 31,300
(212) 408-2513

*Attorneys for Applicant*

BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112